AOIT Computer Networking

Lesson 11

Network Security

Teacher Resources

| Resource | Description |
| --- | --- |
| Teacher Resource 11.1 | Demonstration: Using a Network Monitor |
| Teacher Resource 11.2 | Guide: Network Ports and the Netstat Command |
| Teacher Resource 11.3 | Guide: Configuring a Firewall |
| Teacher Resource 11.4 | Scenarios: Internet Threats |
| Teacher Resource 11.5 | Test: Network Security |
| Teacher Resource 11.6 | Answer Key: Network Security Test |
| Teacher Resource 11.7 | Key Vocabulary: Network Security |
| Teacher Resource 11.8 | Bibliography: Network Security |

Teacher Resource 11.1

Demonstration: Using a Network Monitor

Setting Up a Monitoring Program

Install one of the following network monitors on a network server before beginning Class Period 1:

* Network Monitor is distributed as part of the Windows Server package, but it is not automatically installed; it must be added on. For resources on installing and using Network Monitor for Windows 2003 Server, visit  
  <http://www.windowsnetworking.com/articles_tutorials/Analyzing-Traffic-Network-Monitor.html>
* Wireshark is a free packet sniffing program. For information visit <http://www.wireshark.org>.

For the demonstration, hook up an LCD projector to a network server that has Network Monitor or Wireshark installed.

Demonstration: Teaching Students about Monitoring

During the demonstration, explain to students that there are many reasons to monitor traffic. If the Internet or network is slow, the cause might be a network problem related to hardware or software, or it might be a network security issue such as the following:

* **Denial-of-Service Attacks.** If the network gets inundated with traffic, it could bring a web or email server down. For example, if a company hosts a website that publishes a very popular article, and that article gets linked to from popular sites like BoingBoing, Digg, or Google News, the resulting spike in traffic could crash the server. Malicious hackers may cause a similar problem by inundating a company network with traffic, which prevents other users from logging in.
* **Malware.** If a computer gets infected with malware or viruses, the resulting activity can cause a spike in traffic that slows down the network. Adware, spyware, or viruses could be loading extra programs or trying to infect other parts of the network. An administrator can see where the traffic is originating and try to quarantine or disinfect a compromised client machine on the network.
* **Employee Problems.** A slow network could also be caused by internal problems. It could be an employee downloading files. With monitoring software, the administrator can identify the IP address and computer causing the traffic, and shut down the connection or approach the employee about the issue.
* **Inappropriate Material.** Companies usually have a zero-tolerance policy for inappropriate material and may block certain websites, including social sites like Facebook, or even news and entertainment sites like BoingBoing. Even if sites are not blocked, employees can still be fired or face major penalties for viewing inappropriate content.

Using the network monitoring program, show students how to identify the sources of network traffic and the network speed. In addition, show how network administrators can view which websites employees visit. Explain that sites can be blocked based on their IP addresses or their content. IP address blocking is usually done on routers and works on OSI level 3. Content blocking (based on keywords on a web page) usually uses a proxy server and the filtering is done on OSI level 7. Filtering slows the Internet connection slightly.

Teacher Resource 11.2

Guide: Network Ports and the Netstat Command

Background on Network Ports

Explain to students: Just as a network switch uses hardware ports to connect cables on the network, network services like the Internet and email use network port numbers that allow those services to operate. These ports are special numbers in the header of a data packet that function like an address on the network.

On the board, write some common port numbers for services that students will recognize, such as:

* 53 DNS (Domain Name System)
* 68 DHCP (Dynamic Host Configuration Protocol)
* 80 HTTP (HyperText Transfer Protocol)
* 110 POP3 (Post Office Protocol 3)
* 443 HTTPS (Secure Sockets Layer)
* 5190 AOL Instant Messenger

Explain how ports work: The IP address for the network is like a street address, and the port numbers are something like the room numbers in an apartment building. In order for the data to be sent through the proper services, it needs to contain the correct port number. Like doors, ports can be left open or closed, so that people can easily enter or be blocked from entering.

Using the Netstat Command

Tell students they can check on their computers to find out what ports are open and available by using a simple command, netstat. Write the term *network statistics* on the board and underline *net* and *stat*, to show the origin of the command.

Have students use Internet-connected computers and open a web page, email program, or chat client. Then, have them enter the command prompt and type the command to see all listening ports:   
netstat-an. Let students know that the -a shows all ports, while -n specifies output. Students will see their own address and any foreign addresses they’re connected to. After the foreign address, a colon or period separates the port name or number, as in the following:

* 205.188.8.58.aol
* cf-in-f99.google.http
* localhost.1021

Students will likely see many more protocols and ports than they’re familiar with. Explain that port addresses are 16 bits, so there are 216 ports total, or 65,535 ports. Of those, 1,024 are reserved, well-known ports.

When students perform a netstat scan in their own networks, have them write down additional numbers they discover, perform an online search to find out what the ports are for, and then record their observations in Student Resource 11.2, Worksheet: Network Security.

Teacher Resource 11.3

Guide: Configuring a Firewall

One way to enable a firewall is to use the Security Configuration Wizard to create a new security policy that displays the inbound ports to be opened or blocked and allows for security auditing.

This wizard also isn’t installed by default. You can add it by going to the Control Panel, selecting Add/Remove Windows Components, and then selecting Security Wizard. Once it’s installed, access it by going to the Start menu and selecting Administrative Tools.

The wizard will ask you to open all applications that use network ports so that it can automatically detect the necessary ports. Explain to students that many installations will ask you to close applications, and this is asking just the opposite.

Go ahead and open all such applications, such as Internet Explorer, instant messengers, email clients, or other programs. Then, continue through the wizard.

Under Configuration Action, select “Create a new security policy.” The wizard will create a database of needed server roles and network ports. It will then show a list of the open ports and applications.

Next in the wizard is the audit policy. Explain to students that an audit is a test of network policies and procedures for accuracy and security. The automatic audit in the wizard can be set to monitor successful or failed events to make sure they are functioning smoothly and performing the objective the administrator wants them to.

That should complete the wizard and set up the network firewall.

Further Resources

For more information about configuring the firewall, or troubleshooting, refer to online resources such as the following:

* Troubleshooting Windows firewall with a domain controller: <http://support.microsoft.com/kb/555381>
* Screenshots of running the Security Configuration Wizard: <http://www.windowsecurity.com/articles/Security-Configuration-Wizard-Windows-Server-2003-SP1.html>

Next Steps

Once students have configured their firewalls, they can perform a network statistics scan again and note the ports that have been closed, and record their findings.

Teacher Resource 11.4

Scenarios: Internet Threats

Directions: Make several copies of each scenario and hang them around the room so that students can visit the stations where the scenarios are posted and complete the “What I Learned” column of their worksheet.

Scenario 1: The New Account

Your friend Derek just opened a new credit card so that he can start boosting his credit rating and qualify for a loan to buy a cool new car next year. Soon after he opens the credit account, he gets an email from his bank that says he needs to click a link and verify the password to his account. The email has the bank’s logo and looks legit. So, he opens the link and enters his password in the website that loads up.

But the following month, Derek seems to have a problem with his account. His bank statements stop showing up at his house. When he logs in to his online account to see what’s up, he notices that strange items have been charged to his credit card. It says that he bought a new television and even a new stereo system. Now he has a huge late-payment fee and owes more money than he can afford to pay back!

**What’s the scam?**

Derek is the victim of a classic phishing scam. The email he got was a bogus one—it was from a hacker trying to get his password, not from the bank. The hacker simply copied all the images off the bank’s website and used them to create a new website that looks just like the bank’s, and also created an email that looks like it’s from the bank. When Derek clicked the link in the email, it sent him to this fake website—not his bank’s website. When he entered his password, it was the hacker who received the information, not the bank.

The hacker can use Derek’s information herself or sell it on the black market to identity thieves. ID thieves can use people’s personal information to rack up credit card debt, open new accounts, or even change the address on an existing account.

**What should he have done?**

Derek should have checked that the email was legitimate before clicking the links and entering his password. First, he needs to learn that a bank will never email and ask for his password. Even so, he could have recognized that the email wasn’t real in a couple of ways.

Rather than clicking the link, he could type the bank’s website directly into the navigation bar in his browser. That way, he would be sure to visit the bank’s real site, not a phisher’s site.

Or, he could have checked by calling the bank. He could use Google or his old bank statements to make sure he had the right phone number. (Remember, the phone numbers in an email might be fake, too!)

If Derek had done any of these things, he would have realized that the email was a scam. By notifying the bank about the phishing scam, he might also prevent other people from becoming victims.

**What does he need to do now?**

Now that he knows his bank account is compromised, he needs to dispute the charges in his credit card account and change the address back to his own. He also needs to change all the passwords on his accounts so that the hacker can’t get into any other accounts.

Since the hacker now has Derek’s personal information, he might have opened other accounts with it, too. Derek needs to call the three credit card reporting companies to get a copy of his credit report and check that no harm has been done. If his credit score has been damaged, he might not qualify for a loan to get his new car.

Scenario 2: The Zombie Army

Angie gets an email with some startling news headlines, such as a major storm that killed several people. Soon after, she has more trouble on her hands. Her computer starts responding really slowly, and sometimes she gets strange error messages. Also, her friends have asked her to stop forwarding email messages, even though she hasn’t been sending anything to them.

**What’s the scam?**

Angie is probably a victim of a malware scam called the Storm Worm. This particular email worm is spread through email messages that have interesting headlines like news stories, or e-cards for the holidays. When someone opens one of these messages, the worm gets downloaded onto her computer.

In this case, Angie might not get adware or warnings, because the hacker doesn’t want her to know what’s happening. Instead, he uses all the infected computers on his network like one large super computer. He uses automated scripts—or pieces of code—to do things on the computers.

With these scripts, the hacker can change the user’s settings so that she is sharing more information on the network. He can also forward email to everyone in Angie’s address book. He uses the processing power on her computer for a couple of hours a day. Because her computer is infected, but she doesn’t know about it, it’s known as a zombie computer.

Since the hacker keeps sending emails and infecting new computers, he’s creating a giant network of infected computers. Each of the computers is infected by an automated robot, so it has become a network of robots, and as a whole, this network is known as a botnet. The Storm Worm is a particular botnet that started forming in 2007 and spread quickly worldwide.

**What should she have done?**

Angie should be careful about what emails she opens on her computer. If an email is from a sender she doesn’t recognize, or contains a news headline or other sketchy subject header, she shouldn’t open it.

Additionally, Angie should have antivirus and antimalware software on her computer that can protect her. These software programs work by analyzing the code of malicious software that the developers know about and creating a special block against each of these viruses or types of malware. The code that protects against a virus is called a signature, because it is specific to that virus. But most antivirus software can’t protect against malware, such as adware or spyware.

Additionally, there are always new viruses coming out that antivirus programs don’t have the signatures to protect against yet. So, antivirus software isn’t always effective, and it needs to be updated regularly. That’s why Angie needs to be really careful about what she opens.

**What does she need to do now?**

Angie needs to find the programs that are doing damage on her computer. She can take it to a technician to get it clean, or find software that can help identify and destroy dangerous files.

She can also look in her Task Manager, if she’s using Windows, to find out what processes are happening in her computer. A quick Google search can help her identify which of these tasks are needed for the system and which are foreign and dangerous.

She should also talk to her friends and let them know that they might be infected too, and that they shouldn’t open any strange, forwarded emails from her computer.

Scenario 3: Death and Taxes

Clarisse, an accountant, is getting ready for tax season. She stays up all night at the office, typing numbers into spreadsheets. It’s exhausting work, so at the end of the night, she goes home and crashes out. When she comes in to work the next day, her computer won’t boot up.

Frantically she calls in tech support, and they find out that her hard drive has crashed. All of her data is gone. She’ll have to do all that data entry over again, from scratch!

**What’s the scam?**

In this case, there’s no scam—just poor planning. Hardware gets old, and sometimes it breaks or fails; even if we don’t drop or harm the computer, it will still fail eventually. Network administrators need to keep track of drives and plan for failure by backing up information regularly. All users should also back up their files regularly.

**What should she have done?**

Clarisse should have backed up her files on more than one drive to make sure that if one hard drive failed, she would still have her files intact. She could have emailed the files to herself in an online account, so that it was saved on a web server, or she could have backed it up on a CD, USB drive, or external hard drive. In the best case, she should have backed it up in more than one way, in more than one place. If there’s a fire or natural disaster, that can destroy data too.

In this case, the network administrators are at fault, too. They need to plan so that if a user’s drive fails, the information is saved elsewhere on the network. They can set up a client/server network so that the information is stored on multiple servers—that’s known as redundancy, because the information is stored more than once. They can also set up automatic backups, so that anything on a user’s drive is automatically backed up at the end of the day.

**What does she need to do now?**

Clarisse and the network administrators need to start planning for failure that might happen in the future. They should set up procedures to back up data regularly and save files onto network servers. They might also want to take inventory of their drives and replace any that are old and might fail soon.

Scenario 4: The Pirate Spy

Ronnie is a government spy. He’s always collecting intelligence on the actions of foreign governments and potential terrorists, and keeps most of it on the laptop computer he carries around everywhere.

Ronnie has one weakness: He loves listening to music, and he has turned into a music pirate. He downloads new songs off of peer-to-peer networks on the Internet. Unfortunately, even though he’s a genius spy, he’s not very computer savvy. So, he hasn’t protected any of his confidential information.

All of Ronnie’s personal information, like his tax returns, and his confidential reports on the governments are being kept in the same folder that he’s sharing music from. What he doesn’t realize is that his enemies have discovered that they can download all of his intelligence from his computer while he’s downloading music from other sources on the Internet.

**What’s the scam?**

Ronnie’s enemies can use all of his confidential information against him. If it’s government information, they could use it to plot against the government and plan out a strategy for attack or fraud. If it’s his personal tax documents, they’ll know how much money he has and how he spends it. They’ll also have his Social Security number, so they can open new accounts in his name and rack up a lot of debt.

**What should he have done?**

Ronnie shouldn’t be downloading music off the Net to begin with. First, it’s illegal, and second, he has too much personal information to lose. If he needs to download something off of a peer-to-peer network, he should use a different laptop for his downloads. Or, he could make sure that his Shared folder doesn’t contain critical information, and that all the confidential documents are protected by encryption. If he encrypts the documents, anyone who gets them will need a special code to open them. Even if he doesn’t download music, he should encrypt files anyway, so that if the laptop is stolen, the data won’t be compromised.

**What does he need to do now?**

Ronnie needs to alert the authorities that the information might be compromised. Then, he needs to protect his information in all the ways he should have to begin with. He should also keep close tabs on his bank accounts and credit report, to make sure his enemies aren’t racking up debt in his name.

Teacher Resource 11.5

Test: Network Security

Student Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_

Name two reasons to monitor network traffic, and explain how monitoring can prevent or control a network problem.

Explain one way to block bad traffic from entering a network.

Explain what the netstat command is for and how to use it.

Describe two types of network threats that you might face while browsing the Internet, including how the issues might come up, what consequences they have, and how these threats might be avoided.

Teacher Resource 11.6

Answer Key: Network Security Test

Name two reasons to monitor network traffic, and explain how monitoring can prevent or control a network problem.

Helps administrators stay aware of potential problems and pinpoint the source of adverse traffic, such as a computer spamming other computers, a denial-of-service attack, etc. Also helps administrators stay aware of peak traffic flow and employee misuse of bandwidth (e.g., for video, porn, etc.).

Explain one way to block bad traffic from entering a network.

Ban usage of portable storage devices, block unneeded network ports using a firewall, block pop-ups, etc.

Explain what the netstat command is for and how to use it.

The network statistics (netstat) command shows open and in-use network ports and any addresses the computer is connected to. It can be used to monitor network traffic and identify ports that are open.

Describe two types of network threats that you might face while browsing the Internet, including how the issues might come up, what consequence they have, and how these threats might be avoided.

See Teacher Resource 11.4, Scenarios: Internet Threats, for a full description of some of the network threats that students might mention.

Teacher Resource 11.7

Key Vocabulary: Network Security

These are terms to be introduced or reinforced in this lesson.

| Term | Definition |
| --- | --- |
| adware | A type of malicious software that causes advertisements to pop up on the user’s computer screen. |
| botnet | A network of computers that have been infected by viruses or worms. The computers on a botnet can be used to spam other computers, or their processing power can be harnessed by the hacker and used for illicit purposes. |
| bots | Robots that crawl the web and read the code of web pages, or automated programs that can work behind the scenes on a user’s computer. This is what Google and other search engines use to create an index for search terms. |
| deconstruct | To take something apart in order to understand its underlying structure. In essay terms, this can mean to analyze the outline of the essay or to examine the logical arguments that the writer poses. |
| firewall | A network firewall is used to filter traffic on the network, by blocking unneeded network ports or reading the headers or contents of data packets and determining what is safe or risky based on rules configured by an administrator. |
| floppy disk | An archaic storage device used in the early days of computers to store software or other data; used for spreading the very first computer virus. |
| fraud | Computer hackers can commit fraud by stealing your personal information and using it to impersonate you in order to steal or rack up credit card debt. |
| hacker | Someone who hacks into a computer system in order to steal information or processing power. |
| ID theft | A type of fraud in which someone uses a person’s login, password, or Social Security number to impersonate her and open or change her financial accounts or rack up credit card debt in her name. |
| malware | Malicious software that spreads on a computer network; this can include adware, spyware, or other dangerous computer programs. |
| netstat | A command-line tool used to discover information about network statistics, including open network ports. |
| network port | Special numbers in the header of a data packet that form part of the address for delivering the data packet. This section of the header also indicates what service to use, such as Internet, email, or chat. |
| phishing | A scam in which hackers create a website and an email message that look as if they’re being delivered by a genuine business, in an attempt to trick users into revealing their logins, passwords, or other identifying information. |
| port block | A network security feature where a firewall or other software is used to prevent a service from using certain network ports or physical hardware ports, such as USB devices. This prevents viruses from spreading through those vectors. |
| Social Security number | The number that identifies you to the Social Security Administration, used for tax purposes. This information is often used by banks or other institutions to authenticate or verify users’ identities, so if it falls into the wrong hands, it can be used for ID theft scams. |
| spyware | A type of malware that spies on the user’s actions and reports the information back to the hacker. Spyware can communicate personal information such as passwords; this information can then be used to commit fraud. |
| USB drive | A USB flash drive is a small hard drive that plugs into a computer’s USB port; it can spread viruses or malware between computers. |
| virus | A type of malicious program that replicates itself from machine to machine or onto storage devices. |
| vulnerability | Something in the code of an application or in the physical layout of a network that makes it possible for it to be hacked. |
| zombie computer | A computer that has become infected with malware and performs automated tasks controlled by the hacker. |

Teacher Resource 11.8

Bibliography: Network Security

The following sources were used in the preparation of this lesson and may be useful to you as classroom resources. We check and update the URLs annually to ensure that they continue to be useful.

Print

Lowe, Doug. *Networking All-In-One Desk Reference for Dummies,* 2nd ed. Indianapolis, IN: Wiley, 2005.

Online

Combs, Gerald et al. “Wireshark.” <http://www.wireshark.org> (accessed May 25, 2012).

Hengst, Amy. “Firewall Basics.” Network Security Journal, Tippit, May 25, 2007,  
<http://www.networksecurityjournal.com/features/firewall-basics-052507/> (accessed May 25, 2012).

“How to Configure Windows Server 2003 SP1 Firewall for a Domain Controller.” Microsoft.com, <http://support.microsoft.com/kb/555381> (accessed May 25, 2012).

“How to Install Network Monitor in Windows 2000.” Microsoft.com, <http://support.microsoft.com/kb/243270> (accessed May 25, 2012).

Melber, Derek. “Security Configuration Wizard in Windows Server 2003 Service Pack 1.” WindowsSecurity.com, TechGenix, January 20, 2005, <http://www.windowsecurity.com/articles/Security-Configuration-Wizard-Windows-Server-2003-SP1.html> (accessed May 25, 2012).

Posey, Brien M. “Analyzing Traffic with Network Monitor.” WindowsNetworking.com, TechGenix, June 30, 2005, <http://www.windowsnetworking.com/articles_tutorials/Analyzing-Traffic-Network-Monitor.html> (accessed May 25, 2012).

Skrenta, Rich. “The Joy of the Hack.” Skrentablog, <http://www.skrenta.com/2007/01/the_joy_of_the_hack.html> (accessed May 25, 2012).